AMENDMENTS TO THE DRAWINGS

The attached sheets of drawings include changes to Figures 1, 20 and 21-24, as note below.

In Fig. 1- Please add the legend "PRIOR ART"

Please amend Fig. 21 to denote Figs. 21 A through C.

Please amend Fig. 22 to denote Figs. 22 A through C.

Please amend Fig. 23 to denote Figs. 23 A through C.

Please amend Fig. 24 to denote Figs. 24 A through D.

REMARKS

This is in full and timely response to the Official Action mailed October 5, 2005. Reconsideration and reexamination are respectfully considered.

Drawings

Responsive to the objections to the drawings made by the Examiner, the drawings and corresponding sections of the specification have been variously amended. Specifically, the legend "Prior Art" has been added to Fig.1; the specification has been amended to include a reference to element S257 in FIG. 20; and FIGs. 21-24 have been amended to denote the relevant subfigures, with corresponding amendments made to the references to the subfigures found in the specification. These amendments add no new matter. Applicant respectfully requests reconsideration and withdrawal of the objections to the figures.

Priority Claim

It is also noted with appreciation that the certified copies of the priority documents have been received and acknowledged by the Examiner.

Claims

Claim 14 has been objected to for informality. The claim has been amended to correct the noted disagreement between verb and noun. Applicant appreciates the Examiner's attention to this informality and requests reconsideration and withdrawal of the objection to the claim.

Claims 13, 22 and 35 have been rejected under 35 U.S.C. § 112, ¶2 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

These claims have been amended to recite that "each of said plurality of signature modules respectively executes multiple signature algorithms" which is now more clearly consistent with the independent claims, in that the independent claims indicate that each signature module includes at least one different signature algorithm from the others, and the dependent claims indicate that the individual signature modules may also execute multiple signature algorithms (with at least one being different per the independent claims). Applicant submits amended claims 13, 22 and 35 are recited with the requisite particularity and distinctiveness, and respectfully requests reconsideration and withdrawal of the rejection of the claims under 35 U.S.C. § 112, ¶2.

Claims 1-35 have been rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. This rejection is traversed.

With regard to this rejection, the Examiner states that "[t]he subject matter ... of the claims is not tangible, it appears to be a computer program, *per se*." Applicant notes that none of the claims are drafted in *per se* computer program form. Rather, the claims are to a public key certificate issuing system (1-13), a public key certificate issuing method (14-22), a digital certification apparatus (23-35), and a program storage medium (36). Each of these claim sets recites well-established statutory subject matter, including program storage medium claim 36, which is appropriately drafted as a statutory article of manufacture, and not a computer program *per se*. Moreover, each claim recites tangible, useful subject matter rather than an abstract idea.

For example, claim 1 recites "*A public key certificate issuing system comprising:*

a certificate authority for issuing a public key certificate used by an entity; and

a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;

wherein said certificate authority, having a plurality of signature modules each executing a different signature algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority with reference to a table that associates the registration authority with an assigned signature algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate."

Claim 1 clearly recites statutory subject matter under 35 U.S.C. § 101. With regard to such subject matter, the Court of Appeals for the Federal Circuit, in State Street Bank & Trust Co. vs. Signature Financial Group, Inc., 47 USPQ2d 1596 (Fed. Cir. 1998), states that:

> "... the Supreme Court has acknowledged that Congress intended § 101 to extend to "anything under the sun that is made by man." Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980); see also Diamond v. Diehr, 450 U.S. 175, 182 (1981). Thus, it is improper to read limitations into § 101 on the subject matter that may be patented where the legislative history indicates that Congress clearly did not intend such limitations. See Chakrabarty, 447 U.S. at 308 ("We have also cautioned that courts 'should not read into the patent laws limitations and conditions which the legislature has not expressed.'" (citations omitted))."

State Street, 47 USPQ2d 1600.

Consistent with the expansive view of statutory subject matter, in State Street the court held that calculation of a share price by a computer constitutes statutory subject matter. State Street, at 1601. A recitation of end uses of the share price (*e.g.*, trades, purchases, account management) was not required - the share price itself was a useful, concrete and tangible result.

As another example, a claim to a method for routing interexchange calls that included recitation of a primary interexchange carrier (PIC) indicator in a message record has also been held to be statutory. AT&T Corp. v. Excel Communications, Inc., 172 F.3d 1352, 50 USPQ2d 1447 (Fed. Cir. 1999). As stated therein,

> "[t]he PIC indicator represents information about the call recipient's PIC, a useful, non-abstract result that facilitates differential billing of long-distance calls made by an IXC's subscriber. Because the claimed process applies the Boolean principle to produce a useful, concrete, tangible result without pre-empting other uses of the mathematical principle, on its face the claimed process comfortably falls within the scope of § 101. See Arrhythmia Research Tech. Inc. v. Corazonix Corp., 958 F.2d 1053, 1060, 22 USPQ2d 1033, 1039 (Fed. Cir. 1992) ("That the product is numerical is not a criterion of whether the claim is directed to statutory subject matter.")."

AT&T v. Excel, 50 USPQ2d 1452.

Similarly, Applicant's claimed invention provides a useful, tangible and concrete result in reciting the provision of a public key certificate corresponding to a received public key certification issuance request. There is no independent pre-emption of all uses of underlying mathematical principles that may be used to issue the public key certificate, and no basis for maintaining the rejection of this or any of the pending claims under 35 U.S.C. § 101.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 1-36 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Claims 1-3, 5-6, 8-25, 27, 28, and 30-36 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,659,616 to Sudia ("Sudia") in view of U.S. Pat. No. 6,035,402 to Vaeth et al. ("Vaeth"). This rejection is traversed.

Claim 1 is reproduced above and recites a public key certificate issuing system that comprises a certificate authority for issuing a public key certificate used by an entity and a registration authority that transmits a received request to the certificate authority. The certificate

authority has a plurality of signature modules each executing a different signature algorithm, selects at least one of the signature modules in accordance with the request from the registration authority with reference to a table that associates the registration authority with an assigned signature algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

Various features recited in claim 1 are neither disclosed nor suggested by Sudia and Vaeth, whether taken alone or in combination.

Sudia discloses a method for securely using digital signatures in a commercial cryptographic system, wherein security policy and authorization information are encoded into the signatures and certificates by employing attribute certificates. (Sudia, Abstract). Sudia has no disclosure of any kind regarding a registration authority. Indeed, the Examiner admits that Sudia does not mention a registration authority. (Office Action, p. 5). It follows the Sudia cannot be construed to disclose a system including a registration authority, transmission of a received request from a registration authority to a certificate authority, or selection of one of plural signature modules according to the registration authority associated with the request. Moreover, there is no disclosure or suggestion of selecting a signature module in accordance with a request received from a registration authority, with reference to a table that associates that registration authority with an assigned signature algorithm.

Accordingly, there are quite clearly several features that are absent from Sudia. Vaeth does not remedy the failure of Sudia to disclose such features. Vaeth discloses creation and administration of certificates wherein requests for a certificate are directed to a certificate authority, where they are held and accessed by a registration authority that is said to have verification responsibilities. (Vaeth, Abstract). The registration authority is also referred to as a "virtual" certificate authority in that information required on a certification request data form may be determined by the registration authority, although the form is held at and distributed from the certificate authority. (Vaeth, at 8:3-6). It is not clear how Vaeth can in any way be construed as disclosing or suggesting selection by a certifying authority of a particular signature module from among plural signature modules according to the registration authority that sends a request to the certifying authority. Moreover, since this feature is not even generally disclosed in Vaeth, there quite clearly is no disclosure or suggestion of selecting a signature module with

reference to a table that associates the registration authority with an assigned signature algorithm.

Independent claims 14, 23, and 36 are also neither disclosed nor suggested by Sudia or Vaeth, for reasons similar to those provided regarding claim 1 above.

Since Sudia and Vaeth fail to disclose features that are recited in Applicant's independent claims, whether considered alone or in combination, Applicant submits that the Examiner has failed to produce a prima facie case of obviousness. Also, even if the proposed combination would produce the claimed features, which is not the case, such a combination would be improper as there is no evident motivation to combine the references in the fashion offered by the Examiner. Applicant submits that the Examiner has engaged in an attempt to reconstruct the claimed invention in hindsight, and has failed to set forth a proper basis for an obviousness rejection.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of the noted independent claims as being unpatentable over Sudia in view of Vaeth, as well as the corresponding dependent claims that incorporate the described features and that respectively add their own distinct features.

Claims 4, 7, 26 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Sudia in view of Vaeth, and further in view of U.S. Pat. No. 6,202,157 to Brownlie et al. ("Brownlie"). This rejection is traversed.

Claims 4, 7, 26 and 29 depend either directly or indirectly from the above-described independent claims and thus incorporate the features contained therein. Brownlie discloses a computer network security system. As with Sudia and Vaeth, there is no apparent disclosure or suggestion in Brownlie of a certifying authority that has a plurality of signature modules each executing a different signature algorithm, with the certifying authority selecting at least one of the signature modules in accordance with the request from the registration authority, or of making such a selection with reference to a table that associates the registration authority with an assigned signature algorithm. Thus, the proposed combination would still fail to yield the features incorporated into these dependent claims, let alone the additional features separately recited therein.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 4, 7, 26 and 29 under 35 U.S.C. § 103(a).

For the foregoing reasons, reconsideration and allowance of the claims which remain in this application are solicited. If any further issues remain, the Examiner is invited to telephone the undersigned to resolve them.

Dated:

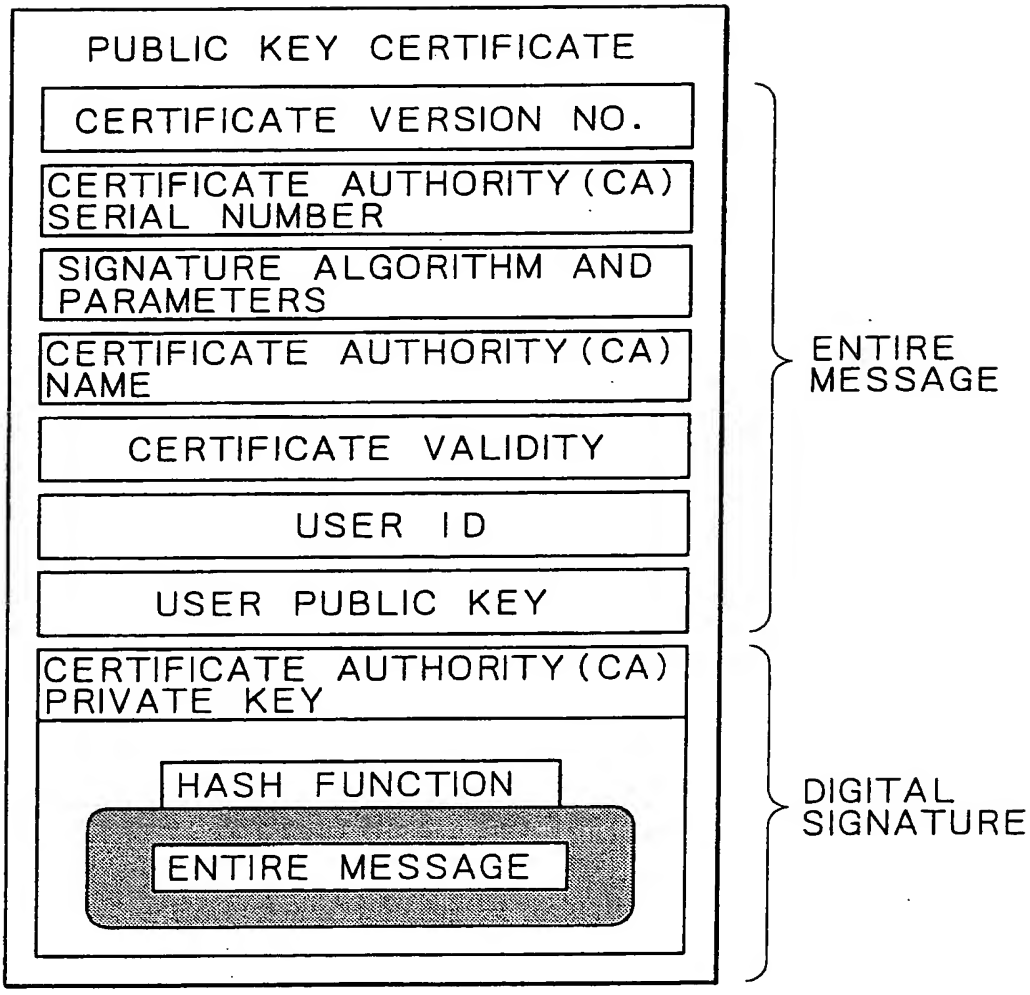
Respectfully submitted,

By _____ 40,290

Ronald P. Kananen
Registration No. 24,104
Christopher M. Tobin
Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W.
Suite 501
Washington, DC 20036
(202) 955-3750
Attorney for Applicant

ANNOTATED SHEET

FIG. 1



Prior Art

FIG. 21A

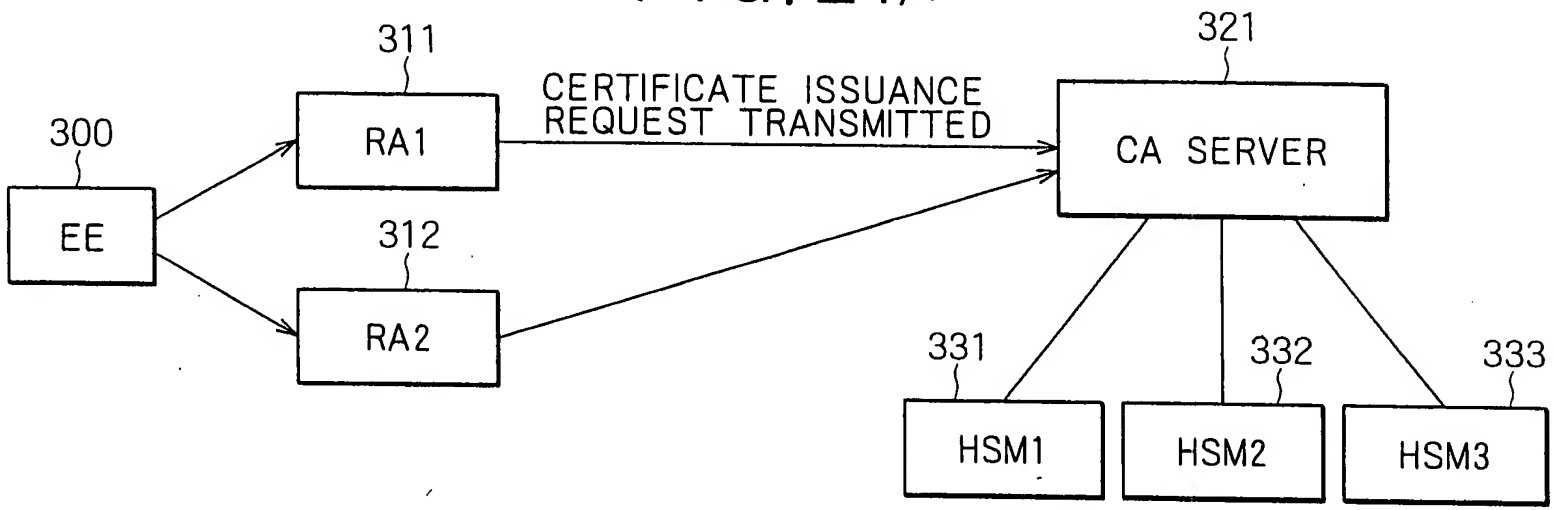


FIG. 21B

(a) RA MANAGEMENT DATABASE

RA ID	USAGE OF MULTIPLE-SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA1	×	RSA	1024 bits	–	×	HSM1
RA2	○	RSA	2048 bits	–	×	HSM2
RA2	○	ECDSA	192 bits	p=XX,...	×	HSM3
RA2	○	ECDSA	192 bits	p=YY,...	×	HSM3

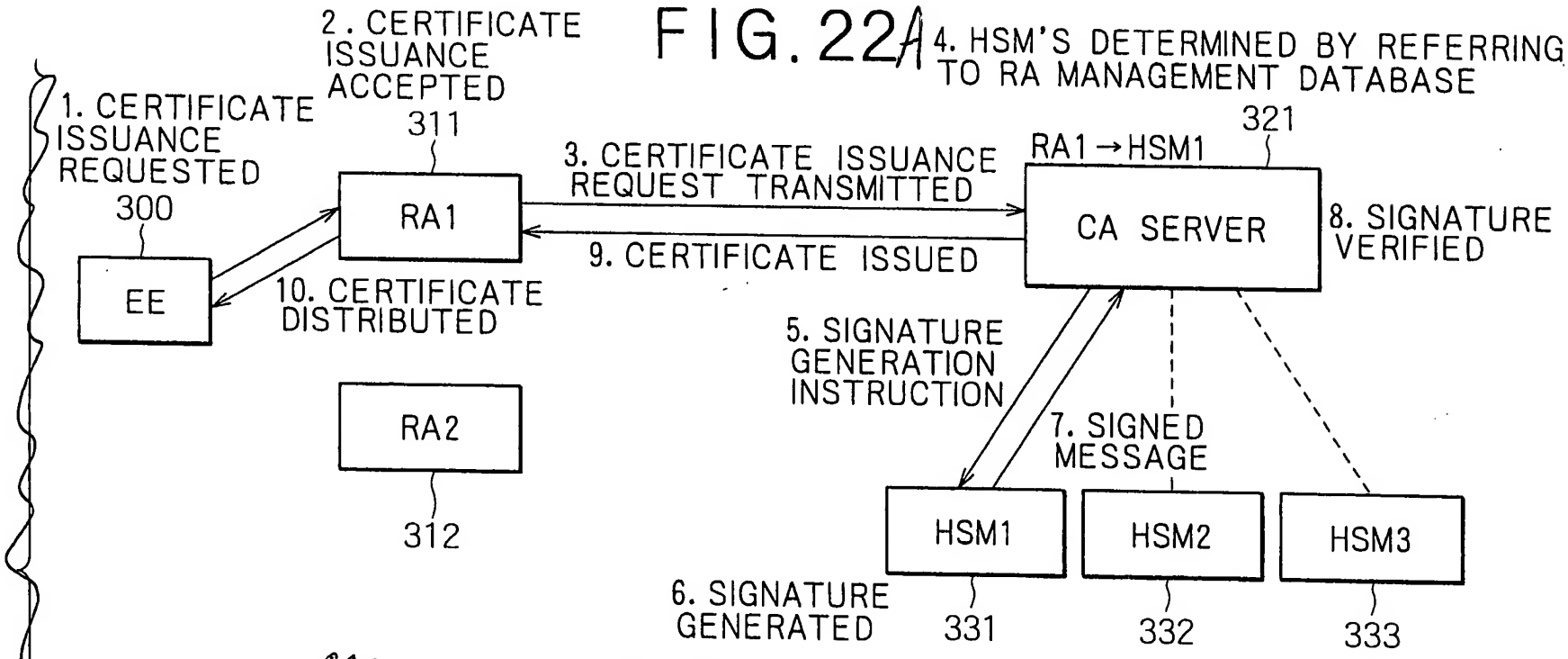
FIG. 21C

(b) VERIFICATION KEY DATABASE

HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
HSM1	RSA	1024 bits	–	◇
HSM2	RSA	2048 bits	–	◆
HSM3	ECDSA	192 bits	p=XX,...	△
HSM3	ECDSA	192 bits	p=YY,...	▲

ANNOTATED SHEET

FIG. 22A



(a) CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID
CERTIFICATE ISSUANCE	Message1	RA2

FIG. 22B

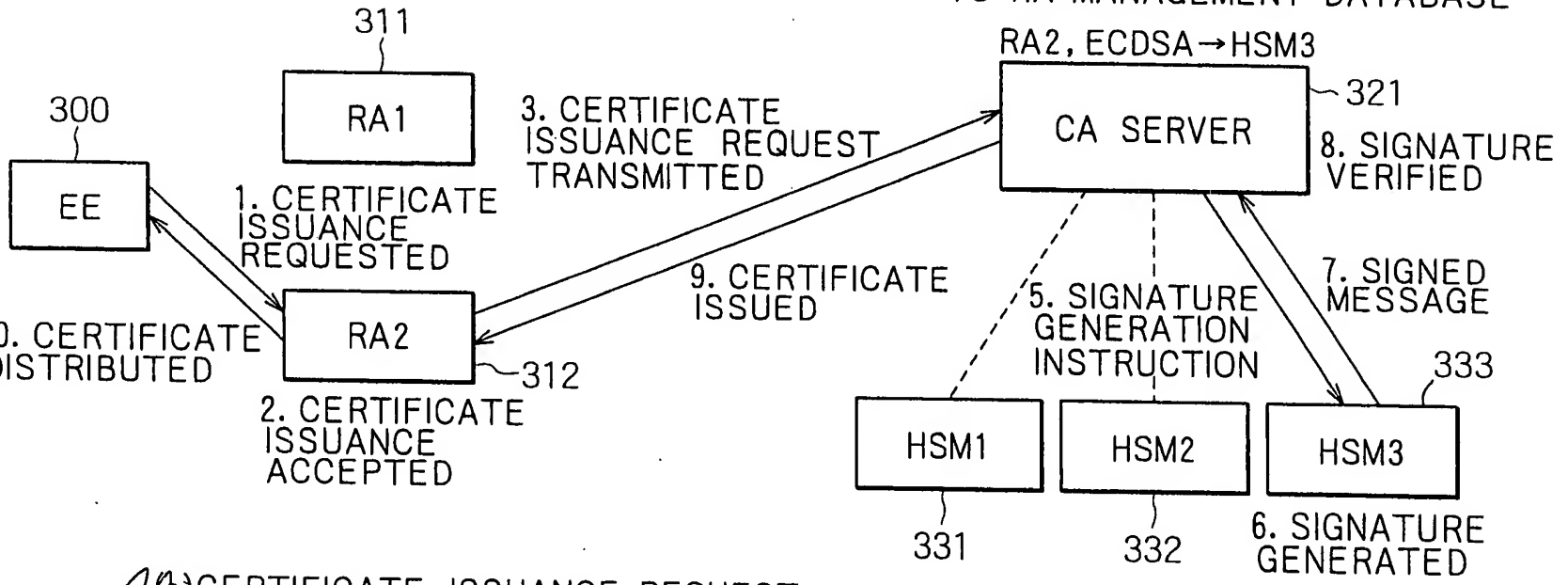
(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE
SIGNATURE GENERATION	Message1

FIG. 22C

ANNOTATED SHEET

FIG. 23A



(a) CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNAL ALGORITHM	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message2	RA2	ECDSA	192 bits	p=XX,...

FIG. 23B

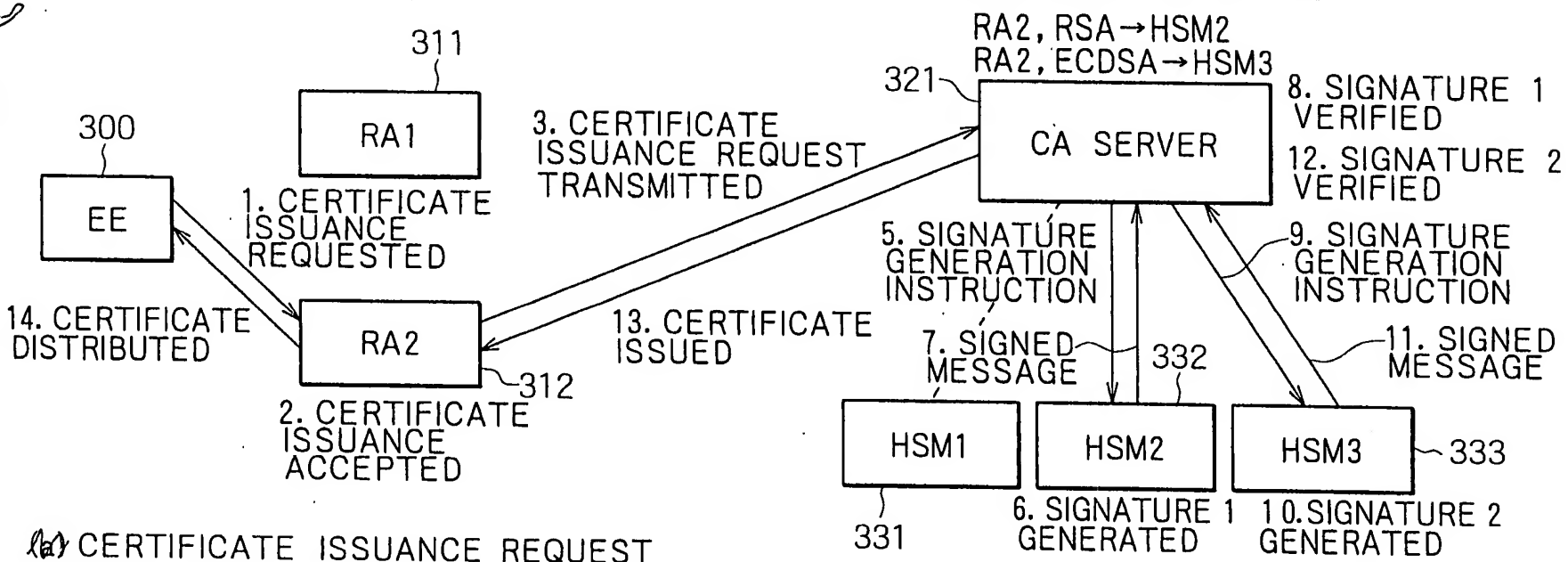
(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message2	192 bits	p=XX,...

Fig. 23C

ANNOTATED SHEET

FIG. 24A



(a) CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNATURE ALGORITHM 1	KEY LENGTH	SIGNATURE ALGORITHM 2	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message3	RA2	RSA	2048 bits	ECDSA	192 bits	p=XX,...

FIG. 24B

(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH
SIGNATURE GENERATION	Message3	2048 bits

FIG. 24C

(c) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message3	192 bits	p=YY,...

FIG. 24D

ANNOTATED SHEET